The collective securitization of cyberspace in the European Union

The European Union (EU) along with the North Atlantic Treaty Organisation (NATO) were forced to radically rethink their common approach to network protection and information security in the aftermath of Russian-sourced, distributed denial of service (DDoS) attacks on Estonian public and private institutions and infrastructure in April-May 2007. Since then, many high-profile cases of cybersecurity breaches and attacks have occurred against EU bodies including against the European Commission, the European Parliament (EP) and the European External Action Service (EEAS). There has also been a steady increase in everyday cyber breaches and greater availability of cyber-disruptive tools online; both problems present a challenge to the growth of the European digital economy (ENISA 2016). It is difficult to find an area of life where Information Communications Technologies (ICTs) are not important, from e-health to social networks to supply chains, cloud computing, The Internet of Things (IoT) and 'smart' systems. The issue of securing cyberspace has thus risen up the EU's political agenda and is perceived as an increasing threat to the EU and to the citizens, governments and businesses of its Member States.

The secure development and use of ICTs is a critical pillar of the EU's Digital Single Market Strategy (European Commission 2015a) and agreed upon initiatives, such as the contractual Public Private Partnership (cPPP) (European Commission 2016a), have been geared

toward stimulating the innovation and competitiveness of Europe's cybersecurity industry.[1] The Cybersecurity Strategy of the European Union (CSSEU) (European Commission and High Representative 2013) identifies five priority areas of action aimed at achieving coherent and effective policies that address threats arising from the increased use of ICTs and the Internet. At the core of this project is the Networks and Information Systems (NIS) Directive. Adopted by the European Parliament in July 2016 and building upon the Directive on Attacks against Information Systems (European Parliament and Council of the European Union 2013), this is the first piece of European legislation that seeks to ensure a minimal institutional capability for reporting cyber incidents across Member States and so manage the risks associated with cyberattacks.[2]

Alongside the CSSEU, the European Agenda on Security (European Commission 2015b) and the Joint Framework on Countering Hybrid Threats (European Commission and European External Action Service, 2016) provide further strategic guidance on cybersecurity and cybercrime. Cyber is also recognised as a priority area in the EU's Communication Launching the European Defence Fund (European Commission 2017a: 3) and is included in the European Commission Communication on achieving an effective and genuine Security Union (European Commission, 2016c). The EU in June 2017, adopted a framework for a joint EU diplomatic response to cyber activities and earlier EU internal security documents and Justice and Home Affairs programmes have referenced the challenges associated with cybersecurity (see Council of the European Union 2010a, 2010b). Perhaps most authoritatively, the EU Global Strategy (Council of the European Union 2016, p.22) points to the importance of fostering a 'common cyber security culture' in order to raise preparedness for cyber disruptions and attacks.

What we have seen emerging in the EU is a system of cybersecurity governance across three distinct, but inter-related mandates: Freedom, Justice and Security (AFSJ), the Internal Market, and the Common Security and Defence Policy (CSDP). These exist within multiple spaces – national, regional and global (Christou 2016). Governance in relation to cyberspace reflects the fact disruption has been framed as a collective threat which, if not addressed effectively through EU rules, norms and regulations will affect the economic and social development of the EU and its Member States. There is thus a clearly articulated sense of 'vulnerab[ility] to cyber incidents' (European Commission 2016b); a view that 'cybercrime is an attack on basic societal values and citizens' security' in the EU (Malmström 2012); and that 'the continuously evolving and deepening threat landscape calls for more action to withstand and deter attacks in the future' (European Commission 2017b). In short, according to the EU's 'Cyber Diplomacy Toolbox' cyber threats present possible harm to the EU's 'political, security and economic interests' (Council of the European Union 2017).

The phraseology of this discourse is worthy of note insofar as it references risk as well as threat (see also Fahey 2014). For the Commission (European Commission 2017b, p.2) there is a 'risk of politically motivated attacks on civilian targets, and of shortcomings in military cyber defence', and an expectation that unless the EU 'substantially improve[s its] cybersecurity the risk will increase in line with digital transformation.' Such framing, has implications for policy and practice. In the case of cybersecurity at the EU level, it can be argued that collective securitization based on a shared understanding of the cybersecurity risk is evolving and visible through the politics of routine rather than through any exceptional measures taken outside 'normal politics.' That is, with cybersecurity, measures taken by the EU have in the main been

reflective of its *modus operandi*, not in exception to it. To extend this further, the inter-changeability of risk and threat in the cyber-security discourse suggests the latter is not a distinct category for which exceptional measures are needed. The cyber-security response, in other words, has been subject to securitisation but that response has obtained a quality of normalcy within the EU.

By way of illustration, a body of EU Regulations, Directives and law has grown relating to cybersecurity (Wessel 2015) and new, more effective governance procedures and agencies have been constituted to address the cross-border, global nature of the cybersecurity problem. This includes the investigation of cybercriminal activity through the European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) (Christou 2018), information sharing through Sectoral Information Sharing and Analysis Centres, and the co-funding of public-private initiatives such as the Online Fraud Cyber Centre and Experts Network. Whilst EU Member State governments still conceive of cybersecurity as a private good to be dealt with through national strategies, they have also recognised that its transnational nature, imbues upon it the status of a collective public good. The central consequence is that cybersecurity threats and risks are shared with others in the EU, with security discourse, practice and policy subsequently evolving and augmenting itself within the EU's rules, norms and procedures to be implemented internally, and projected externally, through the EU's actorness.

It is a central premise of collective securitization (*** and *** this issue), that a logic of securitization is evident when a securitizing actor justifies its actions, and ultimately policy and practice, by reference to an identified threat. In this sense, we can argue that the EU is a securitizing actor in the cybersecurity domain, albeit across a complex ecosystem of

differentiated mandates. Not only this, but we can identify the effects and consequences of collective securitization in relation to governance; that is, increased patterned, stakeholder and regulatory interactions but also in relation to the collective EU effort (or strategy) to address cybersecurity.

This article analyses how the collective securitization of cybersecurity has evolved in terms of the model outlined by *** and *** (this issue). That model's stages are analytically separate but when applied to cybersecurity they are overlapping, messy and interconnected, making systematic presentation somewhat difficult. To add to the difficulty, EU policy itself is fragmented and differentiated temporally across three areas - cybercrime, network and information security, and cyber defence – each underpinned by differing institutional mandates, processes and logics. This makes the identification of the stages of collective securitization more complex in relation to the securitizing actor/audience relationship and in terms of the analysis of national transposition (routinization) in areas where important, newly adopted Directives (e.g. the NIS Directive) have, at the time of writing (April 2018), not been implemented by Member States. That said, the framing article points to collective securitization through aggregation and the articulation of a common EU security discourse despite the EU's many component parts. Such a state of affairs (the EU as actor) can certainly be identified in the case of cybersecurity given the various practices and policies that have sought to address the cybersecurity issue as one that needs to be resolved on an EU wide basis (see also Carrapico and Barrinha 2017).

In order to provide deeper insight in to the collective securitization of EU cybersecurity this article will limit its analysis to two areas - cybercrime and network and information security

(NIS) or critical information infrastructure protection. Cyber defence might seem an obvious focus given that the 'use of cyberspace as a domain of warfare, either solely or as part of a hybrid approach, is now widely acknowledged' (European Commission 2017b, p.2). The EU response here is, however, still under-developed. Cybercrime and NIS are more established and are areas of shared competence where the EU institutions and Member States' actions have increasingly been constructed through a communitarizing process (notwithstanding the tenacity of Member State perspectives in AFSJ). This is pertinent to the collective securitization model and the assumption that a speech act, following a precipitating event or sequence of events and trends, involves statements of authoritative EU actors and endorsement by an empowering audience.

Reflecting a central premise of the collective securitization model, it is argued in this article that both specific events and longer-term trends have galvanised and reinforced the EU discourse of increasing threat and risk around cybersecurity, at different points in time. Thus, for example, whilst the Estonian attacks in 2007 certainly caused the EU to reflect with some urgency on the increasing threat and review its approach, new policy initiatives evolved incrementally thereafter, rather than being the product of any emergency action outside the EU's normal politics. Moreover, it is clear in the case of cybersecurity, that discourses of threat and risk have continued beyond policy initiation, and that this discourse has very much run in parallel with further action and initiatives. Finally, this article demonstrates how collective securitization and legislation in certain key areas related to cybersecurity can also be subject to EU institutional desecuritization moves, leading to national policy differentiation following a precipitating event (e.g. the Edward Snowden affair, which revealed mass surveillance policies).

This article is divided into the following sections. The first provides an overview of how the EU security discourse on cybersecurity has evolved in relation to NIS and cybercrime, and how this has shaped common understandings and governance practices. It will show how a series of events has resulted in securitizing moves, audience response and policy actions that are indicative of a process of collective securitization. In so doing, it will identify instances of recursive interaction between EU Member States and EU institutions that creates a securitization narrative in collective form, and point out what this implies for cybersecurity governance and practice. The second section takes a closer look at recursive interaction and emerging policy and practices specifically around the CSSEU – again, with a focus on NIS and cybercrime. The Conclusion summarises the main implications for the EU as a cybersecurity actor relating to the processes of collective securitization and security governance.

Shaping and transforming the status quo narrative?

No single precipitating event has triggered the EU's policy on cybersecurity; it has, however, evolved in response to identifiable external drivers. The initial EU discourse was underpinned by an economic logic related to the progression of the Single Market. Thus within the Bangemann report (1994) information and computer security was seen as essential to the economic development of the EU and completion of the Single Market (in fact, a concern with the security of computer and information networks in Europe can be traced back still further to the Tengelin Report of 1980). This economic logic has given rise to a number of initiatives relating to cybercrime and the protection of critical national infrastructure.

Network and information security.

The e-Europe initiative (eEurope 1999) and the Communication on Network and Information Security: Proposal for a European Policy Approach, (European Commission, 2001a) highlighted the importance of information infrastructure protection for the EU, with the latter also providing recommendations on how to enhance security within the technical, legal and policy domains. Similarly, the Commission communication Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime proposed a series of measures to address criminal activities both domestically and transnationally, whilst also stressing the need to preserve the balance between security and respect for the fundamental rights of individuals (European Commission 2001b: p.2).

Formatted: Not Highlight

Such Communications, alongside an evaluation of the e-Europe Initiative in 2003, were indicative of a still emergent understanding of cyber security challenges. Hence, there was no mention of computer-related crime or any cyber-related threat in the 2003 European Security Strategy (Council of the European Union 2003). The EU response at this point was, in fact, largely derivative. EU cyber-security discourse in the early 2000s was influenced by frameworks developed by other countries (the US most notably), as well as international and regional organisations such as the G8 (see its Action Plan on computer-related crime, 1997) and the Council of Europe (Convention on Cyber Crime, 2001) (Deflem and Shutt 2006). That said, the EU response did give rise to incipient modes of EU security governance aimed at combating computer crime, and ensuring the reliability and security of networks and information systems. This, in turn, is evidence of the stakeholder interaction noted by *** and *** (this issue). Initiatives driven by EU institutions emphasised the need for cooperation between public and

private stakeholders in response to Member State concerns relating to illegal and harmful content on the Internet and increasing levels of high-tech criminal activity (Council of the European Union, 1997).

The terrorist threats that emerged in the early and mid-2000s facilitated a shift in the perceived vulnerability of information security and network systems within Europe (Carrapico and Barrinha 2017: 13). It was at this time that the economic logic was supplemented by an explicit security logic in the EU's approach to information and network security and computer crime. This, inevitably, had implications for governance practice. In particular, there was a step-change away from a soft law approach (Fahey 2014: 49-51) towards more patterned and regulatory interaction that saw the formulation of legally- binding instruments for addressing attacks on information systems.

Thus, the EU's i2010 initiative (European Commission 2005) emphasised the importance of the security of the Single European Information Space and the 'reliability and security of networks and information systems.' The Council Framework Decision on Attacks against Information Systems, meanwhile, noted:

> There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union (Council of the European

Union 2005).

Similar concerns were expressed on issues of sexual exploitation of children and child pornography giving rise to a 2004 Council Framework Decision (Council of the European Union 2004). That decision stipulated only minimal requirements in terms of approximation of legislation across EU Member States, and subsequently led to problems in prosecuting offenders within and between national borders (Fahey 2014). The legal logic behind these framework decisions, however, was to make coordination of efforts easier between the relevant public authorities (to improve horizontal stakeholder interaction) even if in practice there remained constraints given that there was no real collective culture of cybersecurity.

The European Commission's communication A Strategy for a Secure Information Society (European Commission 2006) and the subsequent, broader Digital Agenda for Europe initiative (European Commission 2010) took coordination further. The former aimed to 'develop a dynamic, global strategy in Europe, based on a culture of security […] founded on dialogue, partnership and empowerment' (European Commission 2006: 3). The Commission recognised that it had to move beyond a focus simply on cybercrime toward network and information security measures and a regulatory framework for electronic communications that addressed issues of privacy and data protection. This meant a multi-stakeholder approach and the promotion of a collective security culture that was more likely to deal not just with the symptoms, but also with the underlying causes of cybercrime, at both individual and institutional levels. While cybersecurity as such had not entered the EU's lexicon at this point – perceptions of increased threats to information and network security had resulted in speech

acts and practice that sought to move beyond the *status quo*.

This shift by the Commission (2006: 6-9) had already been flagged by the creation of the European Network and Information Security Agency (ENISA) in 2004. ENISA would play a key role in identifying best practice, improving awareness, and cultivating partnerships among all stakeholders. It was also tasked in its original mandate (of 2005) with supporting national Computer Emergency Response Teams (CERTs), for which it established a CERT programme and Working Group on CERT Co-operation and Support. One could argue that ENISA was the outcome of an increased awareness of the vulnerability of communication networks and information systems, and the importance of such systems to the economic and societal development of the EU (European Parliament and Council of the European Union 2004). ENISA, in fact, was created – and co-constituted by the Council and EP – because of a growing number of security breaches that had generated substantive damage financially and had undermined confidence, thereby adversely affecting the EU's plans to develop e-commerce. ENISA's raison d'etre was expressed in the language of risk – '[t]o understand better the challenges in the network and information security field, there is a need for the Agency to analyse current and emerging risks' (European Parliament and Council of the European Union 2004: 2). A perception of increased risk thus induced a securitizing move by authoritative EU institutional actors that was accepted by the empowering audience (the Member States). ENISA was granted a second, enhanced, mandate in 2010, and in a subsequent 2017 European Commission proposal for a new Regulation for an EU Cybersecurity Agency (European Commission 2017c: 2) it was suggested ENISA be given 'a more operational and central role in achieving cybersecurity resilience' given 'the prospect of large scale incidents and a possible

Pan-European cybersecurity crisis.' ENISA has had a substantive impact on security governance; for example, in facilitating improved stakeholder interaction (private-private, public-private) and learning and- formulatinge- regulatory compliance mechanisms.

ENISA was only one prong of the EU's emerging approach to critical infrastructure protection. The 2007 cyber attacks on Estonia acted as a trigger for a securitizing move by the European Commission and subsequent agreement and reinforcement by EU Member States. In response to the attacks, the then EU Information Society and Media Commissioner, Viviane Reding (cited in Reuters 2007), asserted that '[w]e have to wake up our governments […] if people do not understand the urgency now, they never will.'. Building on the Council Framework Decision of 2005, the Commission then took the lead (with the caveat that the Member States had provided them with the authority and initiative to do so) in producing a Communication on Critical Information Infrastructure Protection (CIIP) (European Commission 2009), which proposed an action plan to address key challenges. Those proposals sat in parallel to and under the European Programme for Critical Infrastructure Protection (EPICP), and proposals in 2009 to revise the EU's Regulatory Framework for Electronic Communications (European Parliament and Council of the European Union 2009). That revision included legislation that made mandatory (Art.13a) the reporting of any network and information systems security breaches to the national regulatory authority (NRA). This step-change was a significant (framing) move away from the voluntary approach (which had characterised the 2006 Communication, for example), with ENISA tasked to support Member States in implementing Article 13a through the Technical Guidelines on Incident Reporting, which created a standard incident reporting methodology and mechanism (ENISA 2013).

Important in the context of the collective securitization model and increased patterned and stakeholder interaction are the proposed pillars of action in the CIIP: Preparedness and Prevention, Detection and Response, Mitigation and Recovery, International Cooperation, and Criteria for ICT. These pillars have embraced practices relating to the establishment of minimum national level capabilities for CERTs, a European public-private partnership for resilience and a European forum for Member States to share good practice, as well as the establishment of an early warning information sharing and alert system, the development of national contingency plans, and pan-European cyber exercises. Whilst we could frame such proposals as securitizing moves on the part of authoritative EU institutional actors, the extent to which they have resulted in collective securitization in practice is open to debate given that not all Member States have participated equally or indeed implemented symmetrically the proposed pillars of action. Thus, we are missing the co-constitution from the audience in such a move that would routinize practice or indicate policy implementation in this area across all EU Member States. So at best, we can talk of imperfect collective securitization in this instance.

That said, the Member States have shown a willingness to concede an informational if not operational role to an EU agency (principally ENISA) and increased stakeholder interaction has occurred given that certain proposals have been co-constituted by the Commission, ENISA and the Member States. And the Member States in at least one regard - that of cyber-security exercises – have submitted to the coordination of ENISA in what has now become a routine matter. This vertical interaction has been complemented by horizontal initiatives (see *** and *** this issue for this distinction). The 2011 European Principles and Guidelines for Internet Resilience and Stability, was the direct result of horizontal interaction in the European Forum of

Member States (2011) – an EU level body for Member State representatives to share best practice and encourage discussion and cooperation relating to critical information infrastructure security. It set out the principles and norms that would underpin EU policy on internet security and stability. This document, in turn, fed in to the CSSEU (see above) that sets out the position of the EU as an actor in Internet security and stability, and in relation to cybersecurity governance more broadly.

In summary, what we have seen in relation to the EU's approach to CIIP is securitization moves initiated by authoritative EU institutional actors such as the EP, the Council and the Commission following certain specific events and increasing perceptions of threat, risk and vulnerability. The audience (the Member States) has been largely in agreement on broad principles but not always in relation to the specific mechanisms of regulatory security governance (policy output and practice) that might follow.

Cybercrime.

In cybercrime, it has been trends rather than any major precipitating external event that has driven EU initiatives[3] (Fahey 2014; Wessel 2015). The first such trend has been the shift in cybercrime away from simple disruption toward profit seeking. This has meant a proliferation of malware vehicles including spam, spyware and phishing, and an increasing exploitation of compromised servers and computers for their distribution (European Commission 2006: 4). Second, has been technological development. Mobile telephony (mobile based network services) and 'ambient intelligence' (intelligent devices supported by computer and network technology) have presented challenges to the integrity and security of the

Internet, and provided additional platforms for attack by cybercriminals.

The EU was not an institutional first mover in response. The 2001 Framework Decision on Combating Fraud and Counterfeiting and the ePrivacy Directive of 2002 were measures aimed at ensuring the security of electronic communications services and combating fraudulent behaviour. Neither measure focussed on cyber issues to the extent of the European Convention on Cybercrime adopted by the Council of Europe in 2001. That Convention appears, however, to have prompted EU action. In 2005, the EU adopted the Framework Decision on Attacks against Information Systems (Council of the European Union 2005) followed shortly after by the European Commission's Communication Towards a General Policy on the Fight against Cybercrime (European Commission 2007). The latter was crucial in the emergence of new practices and agencies at the EU level. It highlighted '[a] growing vulnerability to cybercrime risks for society, business and citizens' and 'the need for urgent action to improve European coordination and cooperation between high-tech crime units in Member States and with the private sector.'

The approach advocated by the Commission has meant explicit movement towards a type of security governance that entails both non-legal stakeholder interaction (supporting partnership, coordination) and regulatory interaction (legislation to add legal clarity and improve cooperation between law enforcement agencies). This approach, significantly, has had buy-in from the Member States evident in the shaping influence of the EU Internal Security Strategy (ISS) of 2010 and the Stockholm Programme (2010 – 2014) that articulated EU priorities for developing the Area of Justice, Freedom and Security.

Importantly, with regard to the collective securitization model, these initiatives indicate that the Member States had progressed beyond a 'thin' version to imbue the EU with autonomy and agency. The ISS, for instance, recognised 'that many security challenges (cybercrime, terrorism, illegal immigration and organised crime) are cross-border and cross-sectoral in nature', and that 'no single EU country is able to respond effectively to these threats on its own.' The ISS is thus the EU's 'joint agenda to use all the resources and expertise available to jointly tackle these challenges' (EUR-Lex n.d). Such a threat narrative was also reinforced by the European Commission. Its Action Plan for the ISS noted that, '[the] ~~the~~ incidence of attacks against information systems has increased significantly in recent years. Estonia in 2007 and Lithuania in 2008 were subject to large-scale cyber-attack. The botnet 'Conficker' […] has since November 2008 spread to affect millions of computers worldwide, including, in the EU, France, the UK and Germany. Every individual and business using the Internet is potentially vulnerable to cybercrimes' (European Commission 2010).

Cybercrime remains a top priority for the EU. According to the European Commission (2012a: 3), it is a major spur towards 'efforts to develop an overarching EU strategy to strengthen cyber-security.' It is also one of the ten 'most pressing criminal threats' listed in the 2018 – 2021 EU policy cycle for organised and serious international crime (Europol n.d). It might be argued that the resultant security governance (the transposition, execution and routinization of policy down to the Member States) has only been asymmetric at best – limited by 'jurisdictional boundaries, insufficient intelligence-sharing capabilities, technical difficulties in tracing the origins of cybercrime perpetrators, disparate investigative and forensic capacities, scarcity of trained staff, and inconsistent cooperation with other stakeholders responsible for

cyber-security' (European Commission 2012a: 3; see also European Commission 2017d). That said, stakeholder interaction – the deferral to EU institutional prerogatives on cybercrime – has nonetheless occurred. The European Commission has sought to improve cooperation and coordination among national law enforcement agencies, and has promoted legal and political cooperation with third countries, with a particular emphasis on cybercrime training for law enforcement and judicial authorities.

Furthermore, the public-private aspect of the Commission's cybercrime policy has expanded. This has included efforts to combat child pornography, where effective collaboration between credit card companies and law enforcement agencies has assisted police in tracking down users of illegal on-line material. This area has also, however, illustrated a significant limitation on EU action. There is no legal obligation for private companies (i.e. banks and other issuers of credit cards) to share information on cybercrime with public authorities. Secrecy rather than open sharing of information was favoured to avoid threatening the reputation and profits of firms. In this sense, it was the private sector as co-enforcers of agreed practice[4] – despite co-constitution at the EU level of measures to facilitate the combat of cybercrime – that has hindered the realisation of effective outcomes.

The issue of information sharing also has broader ramifications. The EU's agreed rules on data protection, privacy and retention are crucial for the purposes of prosecuting and convicting cyber criminals. The EU has taken forward measures related to operational aspects of cybercrime by implementing the Data Retention Directive (European Parliament and Council of the European Union 2006). As a law enforcement measure aimed at accessing data, this initiative ran up against other measures, notably the Data Protection Directive (European

Parliament and Council of the European Union, 1995) geared toward digital rights and the avoidance of data misuse and surveillance. With the Edward Snowden revelations, data protection has become far more significant and, in effect, the EU has become an agent of desecuritizsation pushing for stronger EU legislation related to data protection and privacy rather than measures to increase intrusion into the private digital space. Even prior to this watershed, the EU had adopted the E-Privacy Directive in 2002 (see above) and an amended version in 2009 with the aim of ensuring the confidentiality of communications and of preventing unauthorised access to customer data. Snowden, however, created a new momentum resulting in the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union 2016), which came into effect in May 2018. A new Regulation on Privacy and Electronic Communications has also been proposed geared toward ensuring 'the […] confidentiality of communications and the protection of personal data in the electronic communications sector' (European Commission 2017e, p.1).

Complementing these desecuritizing moves, in April 2014 the European Court of Justice (ECJ) annulled the Data Retention Directive on the grounds that it represented an infringement of the individual's right to privacy. Such a move, however, has caused considerable tension with certain Member States (the UK, Germany and Portugal) who have mandated data retention. Indeed, in this context the UK's 2016 Investigatory Powers Act, which provides UK security services and police with powers to hack into computers and phones to collect communications data in bulk, has been ruled illegal by the ECJ (Agerholm 2016).

The EU cybersecurity strategy: collective securitization and accelerating security governance?

This section picks out one emblematic initiative – the CSSEU - to illustrate further the significance of the securitisation of cyber by the EU. The CSSEU emerged out of A Proposal on a European Strategy for Internet Security produced by the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). The underlying rationale for that proposal was to deal with a changing threat landscape:

> not only have the Internet and digital technologies become even more central to our economies and societies, but their vulnerability has increased and the number and seriousness of attacks has magnified (attacks on Estonia, on the French Finance Ministry prior to the G20 summit, on the EU Emissions Trading System and most recently on the European External Action Service and the Commission are cases in point) (European Commission 2011: 2).

The CSSEU itself, meanwhile, indicated a move '[t]o address cybersecurity in a comprehensive fashion.' That document acknowledged that 'the complexity of the issue and the diverse range of actors involved' meant 'centralised European supervision is not the answer.' 'National governments are best placed', it continued, 'to organize the prevention and response to cyber incidents and attacks.' That said, 'due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement.' The CSSEU thus went on to provide a clear rationale for an EU role involving a range of bodies (ENISA, Europol, the Commission, the High Representative and others) along with the Member

States in- 'coordinat[ing] international action in the field of cybersecurity.' Interestingly, the CSSEU was the first document to elaborate the need for an EU 'cyberdefence capability' to sit alongside efforts relating to cybercrime and network and information security (European Commission and High Representative 2013). In this sense, it reflected the priorities of those actors within the EU institutional milieu that have been responsible for the development of the different strands of cyber security policy (the influence of the European Defence Agency and the European External Action Service being responsible for the cyber defence component).

It is NIS and cybercrime that will be the main focus of this section given (as noted above) the still formative nature of cyber defence. This is not to argue that horizontal interaction between Member States in cyber defence has been inconsequential, but rather that, the emergence of new practices here (training, education, exercises to test defence capability) are not yet routine or symmetric given there is no obligation (as is the case with Directives, Regulations etc.) to participate, transpose and implement at the national level. This contrasts with NIS and cybercrime. As already noted, each is governed by a mandate which impacts on our understanding of collective securitization and security governance, particularly if we accept the assumption of this Special Issue's framing article that supranational policy is the outcome of recursive interaction and audience acceptance following a securitizing move by a supranational actor(s).

The NIS Directive is illustrative of both a securitization move and the audience's (Member States) acceptance of it. This strand of the CSSEU is underpinned by an Internal Market mandate and subject to the ordinary legislative procedure (OLP). The proposal for the NIS Directive put forth by the Commission was underpinned by a narrative of 'managing

security risks' in the context of a 'fast-changing landscape of threats' based on a view that existing capabilities and mechanisms did not 'ensure a common high level of protection in all the Member States' (European Commission 2013: 1-2). The NIS Directive was adopted after lengthy discussion by the Council in August 2016 (Council of the European Union 2017) (it was accepted by the audience of Member States, in other words). Its aim has been to: advance institutional preparedness among the Member States for cyber events by developing a functioning national/governmental CERT; establish prevention, detection, mitigation and response mechanisms for information sharing and mutual assistance amongst national NIS competent authorities; promote cross-border EU-wide cooperation through an EU NIS Action Plan; and improve the engagement and preparedness of the private sector through the reporting of major NIS incidents to national NIS competent authorities.

In security governance terms, the regulatory logic of the Directive has been to move to mandatory reporting of cyber incidents and attacks given that voluntary, informal measures have proven insufficient to fully engage the private sector. How such security governance practices will become routinized within the EU and how the new strategic vocabulary of cyber security will develop is complicated by the fact that not all actors - - particularly in the private sector – accept mandatory reporting for the creation of an effective culture of cybersecurity. That said, at the time ~~s~~ of ~~this~~ writing it is too early to judge the effectiveness of the Directive (the deadline for its implementation being as recent as May 2018).

Turning to cybercrime, the CSSEU views a dramatic reduction of this problem as a strategic priority and EC3 is singled out as 'the European focal point' in that effort. EC3 was not created against the backdrop of a single precipitating event but rather in response to an

accumulation of problems. Its aim has been 'to protect Europeans and businesses against mounting cyber-threats' (European Commission 2012b). In the words of Cecilia Malmström, European Commissioner for Home Affairs, '[w]e can't let cybercriminals disrupt our digital lives. A European Cybercrime Centre within Europol will become a hub for cooperation in defending an internet that is free, open and safe' (cited in European Commission 2012c). EC3 reflects a desire shared by the Member States, the Council, the Commission and Europol (which is the institutional host) to tackle the increasing threat of cybercriminal activities. These, according to the Europol Serious and Organised Crime Assessment (SOCTA 2013, 2016; see also iOCTA 2016), have included online and payment card fraud, cybercrimes which cause serious harm to their victims (as in online child sexual exploitation), and cyber attacks on information systems and critical infrastructure. EC3 has been tasked with aligning its activities to those of other relevant EU agencies - Eurojust, ENISA, and the European Police College (CEPOL). This is to ensure that the priority areas identified under the EMPACT policy cycle - training, capacity-building, outreach, strategic analysis and technical support - are effectively addressed (see Europol 2014). The EMPACT policy cycle was created by the Council of the EU in 2010 to 'tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU Institutions and EU Agencies, as well as relevant third countries and organizations' (European Commission 2014: 9).

One tangible aspect of EC3 has been the work of its Joint Cybercrime Action Taskforce (J-CAT) established in September 2014 and made up of cyber liaison officers from certain Member States (UK, France, Germany, Spain, Italy, Netherlands, and Austria) and law enforcement partners from outside the EU (Norway, Switzerland, the US, Australia, Canada,

and Columbia). J-CAT has been credited with taking down the RAMNIT botnet (Europol 2015) that had infected 3.2 million computers globally; an operation that brought together and utilized the resources of public and private actors such as Microsoft, CERT-EU, Symantec and AnubisNetworks. J-CAT has received praise for coordinating actions against key cybercrime threats and in recognition of its work, a two-year review led in October 2017 to an indefinite extension of its operational mandate.

J-CAT is subject to a very specific legal framework that allows it to be flexible, providing quick responses through the circumvention of common bureaucratic and legal obstacles. Such practices are not exceptional – but neither are they 'normalized' within the EU system – raising for some commentators, questions relating to transparency and accountability (Christou 2018). That said, in security governance terms, both the EC3 and J-CAT embedded within it have provided a new way of doing things – involving public and private actors, both national and international – that allows for more effective and timely action to be taken against cybercriminals and their networks. In the language of the collective securitization model, what can be identified here is a process whereby cybercrime threat trends have led to speech acts by authoritative EU institutional actors and new measures to tackle them. EC3 and J-CAT are thus good examples of how a collective securitizzation move has resulted in a successful securitization and new security governance practices.

Conclusion

The CSSEU – reviewed and updated in September 2017 by the European Commission – signalled a securitization move which was the culmination not of a one-off event, but rather

cumulative threats to European networks and information systems. Annual cyber threat landscape reports from ENISA indicate how such threat narratives have been sustained in order to ensure such issues do not fall down the EU's agenda. The same goes for European Council Conclusions, and the Commission's reviews of the EU's cybersecurity initiatives and relevant cybercrime and cybersecurity agencies. More broadly, we can see how a changing security environment has given rise to a perception that networks and information systems are increasingly vulnerable. This has promoted the development of security governance platforms, instruments and agencies to address perceived threats to the digital ambitions of the EU. EU policy towards cyber-related crime and networks and information system protection, whilst framed broadly within a security threat narrative, have also emanated from legal and economic logics, (which are still very much present).

A central task of this article has been to demonstrate the visibility of collective securitization within the EU cybersecurity policy space. The focus has been on the NIS and cybercrime specifically given the EU's shared competence in these areas. Consistent with collective securitization we have seen securitizing moves by authoritative EU institutional actors as a result of a series of events and trends, in this case followed by Member State agreement to new legal frameworks, mechanisms and instruments. Further to this, it can be argued that in the areas of cybersecurity there is evidence of actorness – in the sense that the EU has been able to speak and practice security with competence and authority – and, indeed, shape its identity as a cybersecurity actor. EU actorness remains anchored to an aggregating function in that the Member States retain important national prerogatives in the cyber space, but

aggregation has meant a significant movement toward EU autonomy thus indicating the tentative development of the thick version of collective securitisation.

The collective securitization of cyberspace has clearly enabled the EU to carry out the functions of security governance in terms of patterned, stakeholder and regulatory interaction, even if in terms of policy outputs and national transposition, it is not possible to judge at the time of writing, how far new practices have evolved and been implemented/routinized. In cybercrime, the broader EU legal frameworks that have been agreed (for instance, Directives on combating the sexual exploitation of children online, child pornography, and attacks against information systems) have led to the implementation of collaborative practices at national levels between relevant stakeholders, and also transnationally – albeit asymmetrically and with problems remaining relating to consistency, legal clarity and capacity. We can also observe how perceptions of threat, from cybercriminals or in relation to cyber attacks, can result in novel and new governance initiatives (such as the EC3 and J-CAT) alongside the renewal of agencies such as ENISA that deal with the security of networks and information systems in Europe. Indeed, the review of ENISA is indicative of the circular nature of the collective (re)securitization process. Its continuing utility is seen in a context of increasing threat trends (often perpetuated and maintained by the agency as well as other authoritative EU institutional actors) giving rise to a call for an enhancement of its mandate in the EU cybersecurity ecosystem. The implication in all of this is that going forward we need further consideration of differentiated and perhaps also fragmented security governance practices.

Finally, it is worth offering some reflections on the concept of collective securitization and its relationship to security governance in the context of EU cybersecurity. First, the

complexity of cybersecurity has meant that the actor/audience relationship has often been blurred – and co-dependent and securitization moves have been asymmetric across the pillars of cybercrime and NIS. The upshot is that we have not seen an equal evolution of new (and existing) proposed practices. Equally, variation has been evident in the forms of stakeholder interaction that have and are being constituted as a result of collective securitization.

Second, whilst the framework provided by the editors emphasises recursive interaction 'between a security actor (the organisation) and its audience (the organisation's constituent members)' (*** and *** this issue) - there is also a need to consider the 'audience' beyond this, in relation to the implementation and routinization of any new policies that result. This expanded understanding of the relevant audience is especially important where the referents under threat are multiple and where the private sector is essential to both legitimising securitizing moves and the success of any implementation. Moreover, and beyond issues of audience, the role of the private sector in the formulation of regulation, in particular in the field of critical information infrastructure protection (see Carrapico and Farrand 2017), has to be further considered within the collective securitization process.

Finally, we might also ask how contestation following a securitizing move can lead to desecuritizing dynamics (as has been the case with data retention). The collective securitization framework suggests a unidirectional model in which, following a securitizing move and endorsement by the audience, policy implementation occurs. The cybersecurity case has shown, however, that following a precipitating event, agreed legal instruments in the name of collective securitization can be desecuritized by supranational actors such as the ECJ. This has implications, in turn, for the development of security governance. More broadly, we must also

probe further the ethical and normative implications of any securitizing move and practice - for example, how collective securitization sits with collective rights in relation to privacy and data protection. Debates on cybersecurity have shown a real tension here and can (and arguably, should) shape the how practices for enhancing security in cyberspace are developed over time.

References

Agerholm, Harriet (2016). 'Snooper's Charter Dealt Blow after EU's Highest Court Rules "Indiscriminate" Government Retention of Emails is Illegal', *Independent* (21 December), available at: https://www.independent.co.uk/news/uk/politics/snoopers-charter-eu-court-ruling-illegal-investigatory-powers-act-emails-david-davis-a7488041.html (accessed 20 June 2018).

Bangemann Report (1994). Europe and the Global Information Society: Recommendations to the European Council, High Level Group on Information Society.

Bossong, Raphael, and Ben Wagner (2017). 'A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU', *Crime, Law and Social Change*, 67:3, 265–288.

Carrapico, Helena. and André Barrinha (2017). 'The EU as Coherent (Cyber) Security Actor?' *Journal of Common Market Studies*, 55:6, 1-19.

Carrapico, Helena and Benjamin Farrand (2017). 'Dialogue, Partnership and Empowerment for Network and Information Security': the Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers', *Crime, Law and Social Change*, 67:3, 245-263.

Christou, George (2018). 'The Challenges of Cybercrime Governance in the European Union', *European Politics and Society*, 19:3, 355-375.

Christou, George (2016). *Cyber Security in the European Union: Resilience and Adaptability in Governance Policy*. Houndmills, Basingstoke: Palgrave Macmillan.

Council of the European Union (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* 9916/17, Brussels (7.6.2017).

Council of the European Union (2016). *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy,* available at: http://europa.eu/globalstrategy/en (accessed 20 June 2018).

Council of the European Union (2010a). *Internal Security Strategy for the European Union: Towards a European Security Model*, available at: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf (accessed 20 June 2018).

Council of the European Union (2010b). *The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens*, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:jl0034 (accessed 20 June 2018).

Council of the European Union (2005). *Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems,* available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN (accessed 20 June 2018).

Council of the European Union (2004). *Council Framework Decision 2004/68/ JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography,* available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33138&from=EN (accessed 20 June 2018).

Council of the European Union (2003). *A Secure Europe in a Better World: European Security Strategy*, available at: https://europa.eu/globalstrategy/en/european-security-strategy-secure-europe-better-world (accessed 20 June 2018).

Council of the European Union (1997). 'Action Plan to Combat Organised Crime'. *Official Journal of the European Communities*. 15 August 1997. No C 251/1.

Deflem, Mathieu and J. Eagle Shutt (2006). 'Law Enforcement and Computer Security Threats and Measures' in Hossein Bidgoli. *The Handbook of Information Security, Volume 2: Information Warfare; Social, Legal, and International Issues and Security Foundations,* Hoboken, NJ: John Wiley and Sons, 200-209.

Dunn Cavelty, Myria, and Manuel Suter (2009). 'Public-Private Partnerships are No Silver Bullet: an Expanded Governance Model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection* 2: 4, 179-187

ENISA (2016). *ENISA Threat Landscape Report 2016*, ENISA, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (accessed 20 June 2018)

ENISA (2013). *Technical Guidelines on Incident Reporting: Technical Guidance on the Incident Reporting in Article 13a,* Version 2.0, January 2013, available at: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0 (accessed 20 June 2018)

EUR-Lex (n.d). 'Glossary of summaries: Internal Security Strategy', available at: https://eur-lex.europa.eu/summary/glossary/internal_security_strategy.html (accessed 20 June 2018).

European Commission (2017a). *Launching the European Defence Fund*, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* COM (2017) 295 final, Brussels (7.6.2017).

European Commission (2017b). *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, Communication from the Commission to the European Parliament and the Council,* JOIN (2017) 450 final, Brussels (13.9.2017).

European Commission (2017c). *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification (''Cybersecurity Act''),* COM (2017) 477 final, Brussels (13.9.17).

European Commission (2017d). *Report from the Commission to the European Parliament and the Council Assessing the Extent to which the Member States Have Taken the Necessary Measures in Order to Comply with Directive 2013/40/EU on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, COM (2017) 474 final, Brussels (13.9.17).

European Commission (2017e). *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, COM (2017) 10 final, Brussels (10.1.17).

European Commission (2016a). 'Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-threats', 5 July, available at: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (accessed 20 June 2018).

European Commission (2016b). *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* COM(2016) 410 final, Brussels (5.7.16)

European Commission (2016c). *Second Progress Report towards an Effective and Genuine Security Union*, *Communication from the Commission to the European Parliament, the European Council and the Council*, COM(2016)732 final, Brussels (16.11.16).

European Commission (2015a). *A Digital Single Market Strategy for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2015) 192 final, Brussels (6.5.15).

European Commission (2015b). *European Agenda on Security*, COM(2015) 185 final, Brussels (28.4.15), available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (accessed 20 June 2018).

European Commission (2014). *Table on the Implementation of the 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace',* available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0 (accessed 24 March 2014).

European Commission (2013a). *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union*, COM(2013) 48 final, Brussels (7.2.13).

European Commission (2012a). *Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels (7.2.13).

European Commission (2012b). 'Cybercrime: EU Citizens Concerned by Security of Personal Information and Online Payments' (Press Release, July 9), at: http://europa.eu/rapid/press-release_IP-12-751_en.htm?locale=en (accessed 20 June 2018).

European Commission (2012c). 'An EU Cybercrime Centre to Fight Online Criminals and Protect E-Consumers' (Press Release, 28 March), at: http://europa.eu/rapid/press-release_IP-12-317_en.htm (accessed 20 June 2018).

European Commission (2011). 'Proposal on a European Strategy for Internet Security', November 2011.

European Commission (2010). *A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* COM (2010) 245 final/2, Brussels (26.8.10).

European Commission (2009). *Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience, Communication on Critical Information Infrastructure Protection from the Commission to the European Parliament,*

the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2009) 149 final, Brussels (30.3.09).

European Commission (2007). *The Commission Communication "Towards a General Policy on the Fight against Cyber Crime",* MEMO/07/199, Brussels (22.05.07).

European Commission (2006). *A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2006) 251, Brussels (31.5.06).

European Commission (2005). *i2010 - A European Information Society for Growth and Employment, Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee* COM(2005) 229 final.

European Commission (2001a). *Network and Information Security: Proposal for a European Policy Approach*, COM(2001) 298 final, Brussels, (6.6.01).

European Commission (2001b). *Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-related Crime*, COM(2001) 890 final, Brussels, (26.1.01).

European Commission and European External Action Service (EEAS) (2016). *Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union Response,* 6 April, JOIN(2016) 18 final.

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy / Vice-President of the Commission (2013). *Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace*, Brussels, JOIN (2013) 1 FINAL, (7.2.13).

e-Europe (1999). *An Information Society for All. Communication of 8 December 1999 on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000* COM(1999) 687 final, Brussels (8.12.99)

European Forum of Member States (2011). *European Principles and Guidelines for Internet Resilience and Stability*, version of March 2011, available at: http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf (accessed 20 June 2018).

European Parliament and Council of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation), OJ 2016/L 119/1.

European Parliament and Council of the European Union (2013). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*

European Parliament and Council of the European Union (2009). *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 Amending Directives 2002/21/EC, 2002/19/EC and 2002/20/EC.*

European Parliament and Council of the European Union (2006). *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks (annulled by ECJ in Case number C-293/12, 8 April 2014).*

European Parliament and Council of the European Union (2004). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency.*

European Parliament and Council of the European Union (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.*

Europol (2014). *European Cybercrime Centre (EC3): First Year Report*, available at: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report (accessed 20 June 2018).

Europol (2015). 'Botnet Taken Down through Internal Law Enforcement Cooperation', press release, 25 February 2015, available at: https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation (accessed 20 June 2018).

Europol (n.d.). 'EU Policy Cycle – EMPACT', available at: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact (accessed 20 June 2018).

Fahey, Elaine (2014). 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation* 5(1): 46-50.

iOCTA (2016). *The Internet Organised Crime Threat Assessment Report*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (accessed 20 June 2018).

Malmström, Cecilia (2012). Public-Private Cooperation in the Fight against Cybercrime, Speech/12/409. Available at: http://europa.eu/rapid/press-release_SPEECH-12-409_en.htm (accessed 20 June 2018).

Reuters (2007). 'Attack on Estonia puts Cyber Security on EU Agenda', Internet News, July 3 2007. Available at: https://uk.reuters.com/article/oukin-uk-eu-digital/attack-on-estonia-puts-cyber-security-on-eu-agenda-idUKL3044463420070630 (accessed 20 June 2018).

SOCTA (2013, 2016). *The Serious and Organised Crime Threat Assessment*, available at https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2 (accessed 20 June 2018).

Wessel, Ramses. A (2015). 'Towards EU Cybersecurity Law: Regulating a New Policy Field', in Nicholas Tsagourias and Russell Buchan (eds.) *Research Handbook on International Law and Cyber Space*, Cheltenham: Edward Elgar Publishing, 403–25.

Endnotes

[1] For a conceptual exploration and critical discussion of the role of Public-Private Partnerships in EU cybersecurity see Bossong and Wagner (2017). See also Dunn Cavelty and Suter (2009) on PPPs and Critical Infrastructure Protection.

[2] A mandatory requirement to report network and information security breaches was included in the revised EU Electronic Communications Regulatory Framework in 2009 (European Parliament and Council of the European Union 2009). This requirement (Art.13a, Directive/140 EC) was restricted to the telecommunications sector, however, whereas the NIS Directive broadened the scope to a wide array of actors involved in network and information security.

[3] The EU's discourse and policy on cybercrime has also borrowed from existing national, international and regional frameworks such as the Council of Europe Conference on Criminological Aspects of Economic Crime (1976), the US Crime Control Act (1984) and the Computer Fraud and Abuse Act (1986). See Deflem and Shutt (2006) for a detailed account of the evolution of computer crime legislation.

[4] An interesting perspective on the role of private actors as important regulators in themselves (as opposed to just co-enforcers) in the area of EU critical information infrastructure is provided by Carrapico and Farrand (2017).